Humboldt-Universität zu Berlin
Institut für Informatik
Rechnerorganisation und Kommunikation

Spezielle Techniken der Rechnerkommunikation

Leitung: Dr. Siegmar Sommer

ZigBee

A Wireless Personal Area Network

Daniel Apelt, apelt@informatik.hu-berlin.de

Jörg Pohle, pohle@informatik.hu-berlin.de

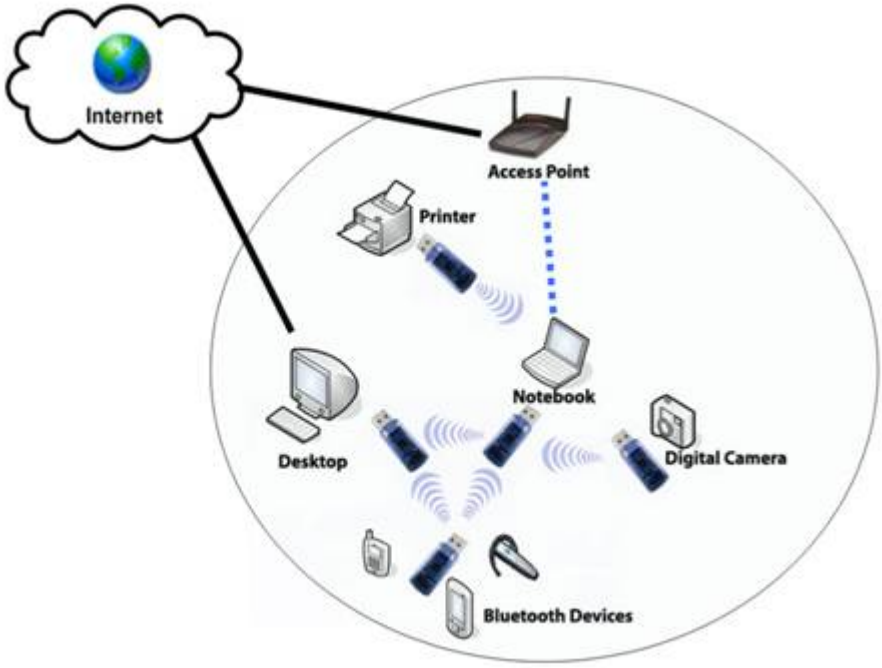
---

19. Juli 2006

Inhaltsverzeichnis

1 (Wireless) Personal Area Networks

Personal Area Network sind, wie der Name schon sagt, personenbezogene Netzwerke. Wobei sie nicht personenfixiert sind und völlig unabhängig von Personen funktionieren. Personal Area Networks (PAN) haben eine Reichweite von wenigen Zentimetern bis 50 m und sind damit die kleinsten Netzwerke der Netzwerkhierarchie. PAN werden in der Regel ad-hoc auf- und abgebaut. Sie werden für die direkte Kommunikation von Geräten untereinander und zur Kommunikation mit einem höheren Netzwerk genutzt. Als direkte Kommunikation von Geräten untereinander wird die Anbindung und Ankopplung von Peripheriegeräten (Tastatur, Maus, externe Speicher etc.) und die direkte Vernetzung von Computern bezeichnet.



http://anmc.postech.ac.kr

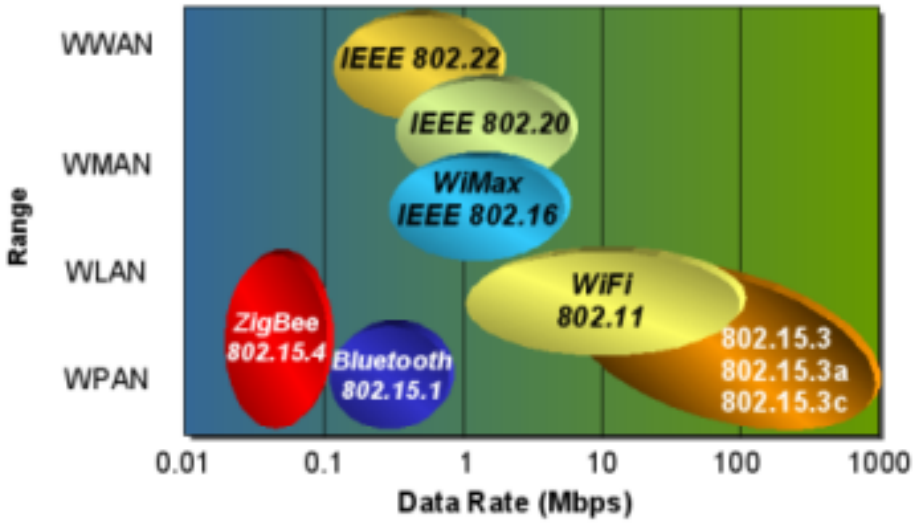
Unterscheidung PAN und WPAN

Personal Area Networks teilen sich in drahtgebundene und drahtlose PANs. Die drahtlosen PANs werden Wireless Personal Area Networks genannt.

Beispiele für drahtgebundene Personal Area Networks sind USB und Firewire IEEE 1394. Gängige Wireless Personal Area Networks sind IrDA und Bluetooth. In Entwicklung bzw. kurz vor der Markteinführung sind ZigBee und Wireless USB.

Im Gegensatz zu Wireless Local Area Networks (WLAN) arbeiten Wireless Personal Area Networks mit geringerer Sendeleistung. Dies führt zu einer Energieersparnis und damit, bei mobilen Geräten zu einer verlängerten Batterie-

und Akku-Lebensdauer. Durch ihre niedrigere Sendeleistung sind Störungen für Dritte geringer. Gleichzeitig verlieren Störungen durch Dritte auf Grund der kurzen Reichweite an Bedeutung. Typischerweise sind bei WPAN auch geringere Datenübertragungungsraten als bei WLAN zu finden. Mit der Einführung von Ultrabreitband als Trägertechnologie wird dies allerdings nicht mehr so sein. Die folgende Grafik zeigt die Reichweite bezogen auf die Netzwerkhierarchie und die Datenrate der einzelnen drahtlosen Technologien.



http://www.zigbee.org/en/resources/

WPAN sind nicht zwingend auf Funkwellen als Träger angewiesen. Das weit verbreitete und etwas ältere IrDA (Infrared Data Association) nutzt Infrarot im Bereich 850 - 900 nm als Träger und bringt es auf bis zu 16MBit/s. Allerdings ist bei IrDA eine Sichtverbindung notwendig. Im Vergleich dazu bringt es das aktuelle Bluetooth 2.0 auf max. 2,1 MBit/s.

Standards

Die Standardisierung wird von der IEEE 802.15 working group für Wireless Personal Area Networks vorangetrieben. Die working group besteht aus mehreren Task Groups und Kommittees. Die working group beschäftigt sich in der Regel nur mit Standards der MAC- & PHY-Ebene.

Task Group 1: erstellte WPAN-Standard (802.15.1) auf der Basis von Bluetooth 1.1, derzeit inaktiv

Task Group 2: erarbeitete Vorschläge (802.15.2) zur Koexistenz von WPAN und WLAN im freien Frequenzband, derzeit inaktiv

Task Group 3: die für High-Rate WPAN (802.15.3) zuständige Task Group, mit 802.15.3a sollte ein Standard für Ultrabreitband (UWB) entwickelt werden, derzeit ist nur die 3c aktiv, sie erarbeitet einen Standard für eine auf Millimeter-Wellen (57 - 64 GHz) basierende PHY-Schicht, Datenraten von bis zu 2 GBit/s sollen damit möglich sein

Task Group 4: Standard für Low-Rate WPAN mit geringem Energiebedarf und einfacher Bauweise (802.15.4), ZigBee basiert darauf, derzeit werden Alternativen auf Basis von Ultrabreitband (802.15.4a) und Erweiterungen für den ursprünglichen Standard (802.15.4b) erarbeitet

Task Group 5: beschäftigt sich mit WPAN Mesh Networking (802.15.5)und den damit notwendigen Änderungen

SCWng: das Standing Committee Wireless Next Generation beschäftigt sich mit neuen Technologien im Bezug auf eine mögliche Standardisierung innerhalb von IEEE 802.15 und ist nicht auf die MAC- & PHY-Ebene beschränkt

2 (W)PAN-Technologien

2.1 Ultrabreitband

> Als Ultra Wide Band wird jede Funktechnik bezeichnet, die eine Bandbreite von mehr als ein Viertel ihrer Mittenfrequenz oder mehr als 500 MHz abdeckt.[1]

Ultrabreitband (UWB) ist eine pulsbasierte Funktechnik die ihre Wurzeln im späten 19. Jahrhundert hat. Die Informationen werden nicht mehr auf einen Träger moduliert, sondern es werden Pulse gesendet, die eine grosse Bandbreite nutzen. Die potentielle Datenrate über UWB ist proportional zur Bandbreite des Kanals und dem Logarithmus des Signal-Rausch-Verhältnis (Shannons Gesetz).

Nach der o.g. Definition gilt damit als UWB wenn mit einer Mittenfrequenz von 1 GHz und einer Bandbreite von 250 MHz gesendet wird. Die Mittenfrequenz ist das geometrische Mittel der genutzten Frequenzen, da die Frequenzverteilung logarithmisch ist.

Ultrabreitband ist auf Grund der Nutzung eines grossen Teiles des Frequenzspektrum nur für WPAN, aber nicht für höhere Netzwerke wie WLAN geeignet. Damit andere Frequenzen und die darauf basierenden Dienste nicht in Mitleidenschaft gezogen werden, hat die Federal Communications Commission der USA (FCC) einige Regelungen für die Nutzung von UWB-Geräten erlassen. Geräte die mit UWB senden, dürfen eine maximale Sendeleistung von 1 mW haben. Desweiteren wurde der nutzbare Frequenzbereich auf 3,1 - 10,6 GHz und die Leistung pro Frequenz auf -41,25 dBm/MHz beschränkt. Diese Beschränkungen sind vor allem für die Dienste wichtig, deren Signale kurz über der Rauschgrenze liegen (GPS) oder deren Frequenzbereich schon stark belastet ist (WLAN, GSM).

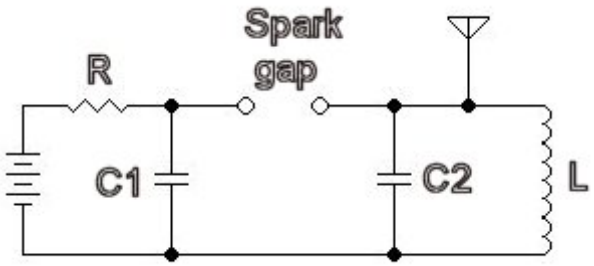
WPAN über UWB benötigt 1-2 Giga-Pulse/s. Für Radar, Imaging sowie Positioning hingegen werden nur 1-10 MegaPulse/s benötigt.

Geschichte der Funkentechnik

Die dem Ultrabreitbandfunk zu Grunde liegende Technik wurde erstmalig 1886 von Heinrich Hertz praktisch umgesetzt. Ein Kondensator entlädt sich über eine

[1] http://www.intel.com/technology/ultrawideband/downloads/Ultra-Wideband_Technology.pdf

Funkenstrecke (Spark gap). Beim Überschlag des Funken wird das breite Spektrum an hochfrequenter Energie genutzt, um es über eine Antenne abzustrahlen. Für mehrere gleichzeitige Übertragungen funktioniert dies natürlich nicht, da sich dann die Sender gegenseitig überlagern. Dieses Prinzip wurde von Marconi kommerziell verwertet. Marconi baute damit die erste drahtlose Nachrichtenkommunikation über den Ärmelkanal und später über den Nordatlantik. In den 1920ern wurde diese Art von Nachrichtenübertragung verboten, da sie das damals aufkommende schmalbandige Radio massiv störte. Militärisch wurde dieses Prinzip allerdings weiter verwendet - seit den späten 1930ern als Radar.



http://en.wikipedia.org/wiki/Spark-gap_transmitter

2.1.1 Technische Grundlagen

Orthogonal Frequency Division Multiplexing

Orthogonal Frequency Division Multiplexing (OFDM) nutzt statt eines einzelnen Trägers eine große Anzahl an Subträgern. Bei OFDM werden die drei Parameter Frequenz, Amplitude und Phase für die Kodierung Information verwendet. Die Symboldauer ist bei OFDM sehr viel länger als bei Einträgerverfahren, da eine gleichzeitige Übertragung der Daten stattfindet. Das Signal liegt als länger in der Luft, dadurch kann für jeden Subträger ein eng begrenztes Frequenzband genutzt werden. Alle Subträgerfrequenzen stehen orthogonal zueinander. Dadurch können die Signale mit komplex rechnenden inversen diskreten Fouriertransformationen (IDFT) von digitalen Signalprozessoren erzeugt werden. Der Hochfrequenzteil bleibt dadurch relativ einfach und kann billig und mit wenig Aufwand prodziert werden. Beim Empfänger wird das Signal über eine Fast-Fouriertransformation dekodiert.

Direct Sequence Spread Spectrum

Die Datensignale werden auf einem breiten Frequenzband übertragen. Das Ausgangssignal wird hierbei mit einer vorgegebenen Bitfolge (Chip-Sequenz) gespreizt. Der Empfänger kennt die Chip-Sequenz und kann damit das ursprüngliche Sigal wieder herstellen. Diese Technik ist unanfällig für Störungen durch Interferenzen, da schmalbandige Störsignale unterdrückt werden.

2.2 Weitere (W)PAN-Technologien

Die in den weiteren Kapiteln vorkommenden Technologien, werden hier kurz erläutert. Sie wurden fast ausnahmslos schon in der Vorlesung „Grundlagen der

Rechnerkommunikation“ behandelt.

2.2.1 Quadratur Phase Shift Keying

Quadratur Phase Shift Keying (QPSK) ist eine Kodierung über die Phasenverschiebung (Phase Shift). Bei der QPSK werden vier Phasenwerte pro Symbol kodiert, damit sind pro Symbol 2 Bits übertragbar. Eine bekannte Anwendung für QPSK ist die FAX-Übertragung.

2.2.2 Quadraturamplitudenmodulation

Hierbei wird das Trägersignal Phasen- und Amplitudenmoduliert. Es ist somit eine Kombination aus QPSK und Amplitudenmodulation. Bei QAM-16 werden beispielsweise vier Phasen- und vier Amplitudenwerte pro Symbol kodiert. Damit sind pro Symbol 4 Bits übertragbar. Eine bekannte Anwendung für QAM ist die Übertragung der beiden Farbdifferenzsignale beim analogen Fernsehen.

2.2.3 Carrier Sense Multiple Access with Collision Avoidance

Bei diesem Verfahren wird keine Kollisionenerkennung gemacht, da Kollisionen unter Umständen auch nicht erkannt werden können (hidden station Problem). Es wird eine Trägererkennung durchgeführt und bei freiem Träger bzw. Kanal wird gesendet. Gleichzeitig startet der Sender einen Timeout. Wenn innerhalb des Timeout kein Bestätigungsrahmen des Empfängers kommt, wird die Übertragung nach dem Abwarten einer zufälligen Zeit wiederholt.

2.2.4 Time Division Multiplexing/Time Division Multiple Access

Time Division Multiplexing (TDM) unterteilt die Übertragungszeit in Zeitabschnitte. Die freien Zeitabschnitte werden zur Übertragung von Datenteilen einer Verbindung unter Nutzung der gesamten Bandbreite verwendet. Beim synchronen TDM werden die Zeitschlitze fest einer Verbindung zugeordnet. Dadurch wird unter Umständen ein leerer Abschnitt übertragen. Beim asynchronen TDM werden die Zeitschlitze nicht fest einer Verbindung zugeordnet, sondern den Verbindungen, die gerade Daten übertragen wollen. Im Unterschied zu TDM kommen bei Time Division Multiple Access (TDMA) mehrere Sender und Empfänger zum Einsatz.

2.2.5 Fehlerkorrekturmassnahmen

1/3 Forward Error Correction

Jedes einzelne Bit wird dreimal hintereinander übertragen: b0 b0 b0 b1 b1 b1 b2 b2 b2 b3 b3 b3

2/3 Forward Error Correction

Das ist eine Hamming-Kodierung um 10 Bit Nutzdaten in 15 Bit zu codieren. Dadurch können 1-Bitfehler korrigiert und 2-Bitfehler erkannt werden.

Automatic Repeat Request

Automatic Repeat Request (ARQ) versucht durch Sendewiederholung eine zuverlässige Datenübertragung zu gewährleisten. Dabei wird ein Datenpaket solange wiederholt, bis eine positive Quittung empfangen oder ein Timeout überschritten wird. Bekannte Verfahren sind Stop-and-Wait, Go-Back-N und Selective Repeat ARQ.

2.2.6 ISM-Band

Das ISM-Band ist keine Technologie, aber durch die zum Teil weltweite freie Nutzung iste es die Grundlage vieler drahtloser Anwendungen. Das Industrial, Science and Medical-Band sind lizenzfreie Frequenzbereiche für Hochfrequenzgeräte. In diesen Bereichen müssen meist nur Auflagen bezüglich der Sendeleistung und Störung benachbarter Frequenzbereiche eingehalten werden. Die Frequenzbereiche für ISM liegen im Bereich von 6780 kHz bis 245 GHz (Mittenfrequenz). Derzeit von WPAN genutzte Bereiche sind 2,4 - 2,5 GHz (Mittenfrequenz 2,45 GHz, weltweit), 902 - 928 MHz (Mittenfrequenz 915 MHz, nur Nordamerika) und 868 - 870 MHz (nur für Short Range Devices, nur Europa, besondere Regelungen). Durch die lizenzfreie Nutzung sind einige Bänder wie das 2,45 GHz-Band schon stark genutzt, so dass es häufig zu Störungen kommt.

3 Bluetooth

3.1 Geschichte

Bluetooth ist benannt nach Harald I. Blauzahn Gormson (Harald Blåtand), einem dänischen Wikinger-König. Er eroberte Norwegen und vereinte es mit Dänemark. Für die Christianisierung der Dänen war er massgeblich verantwortlich. Da Blåtand Dänemark und Norwegen einte, wurde sein Name gewählt um Mobiltelefone mit ihren Peripheriegeräten zu „einen“.

Im Jahre 1994 gab es eine Studie von Ericsson zur Machbarkeit einer Kurzstrecken-Funkverbindung im Handy als Ersatz für die bisherigen Kabel mit den versch. Steckern. Ein Pluspunkt gegenüber dem damals schon existierenden IrDA war die nicht notwendige Sichtverbindung. Dieser Idee schlossen sich alsbald einige Firmen an, so dass im Jahre 1998 die Bluetooth Special Interest Group (SIG) mit Ericsson, IBM, Intel, Nokia und Toshiba als Gründungsmitlgiedern ihre Arbeit aufnehmen konte. Heute hat die Bluetooth SIG über 1.800 Mitglieder. Im Juli 1999 wurde Bluetooth 1.0 als Standard verabschiedet. Er spezifizierte einen kompletten Protokollstack von der Bitübertragungsschicht bis zur Anwendungsschicht. Der später verabschiedete und auf Bluetooth 1.1 aufbauende Standard IEEE 802.15.1 definierte nur die Bitübertragungs- und Sicherungsschicht.

3.2 Designziele

Bluetooth wurde unter den folgenden Prämissen entwickelt:

- Sprach und Datenunterstützung
- Ad-hoc-Konnektivität
- Interferenzresistenz (im ISM-Band 2,45 GHz befindet sich einiges)

- weltweit nutzbar
- Sicherheit (Kabel als Maßstab)
- geringe Grösse, damit in möglichst viele Geräte integrierbar
- geringe Leistungsaufnahme
- preiswert

3.3 Technologie

Bluetooth nutzt im ISM-Band 2,45 GHz den Bereich von 2,402 - 2,480 GHz mit 79 Frequenzstufen bei einer Kanalbreite von 79 MHz. Zur Verbesserung der Interferenzresistenz nutzt Bluetooth ein adaptives Frequenzhopping über die 79 Frequenzstufen. Dabei finden bis zu 1.600 Frequenzwechsel/s statt. Sobald eine Frequenzstufe angesprungen wurde die gestört ist, wird diese eine Zeitlang nicht mehr angesprungen. Bluetooth ist ein Niedrigenergiesystem mit einer spezifizierten maximalen Stromaufnahme von 140 mA und drei verschiedenen Sendeklassen (1 mW, 2,5 mW, 100 mW). Die Gesamtdatenrat ist bei Bluetooth 2.0 mit 2,1 MBit/s spezifiziert. Bluetooth nutzt die schon oben genannten 3 Arten der Fehlerkorrektur: 1/3 Forward Error Correction, 2/3 Forward Error Correction und Automatic Repeat Request. In den zukünftigen Versionen von Bluetooth soll einerseits die Sicherheit verbessert und der Energieverbrauch gesenkte werden sowei die Nutzung von UWB als PHY-Schicht eingeführt werden.

Piconet / Scatternet

Die Grundstruktur bei Bluetooth ist das Piconet. Darin können maximal 8 Geräte (1 Master, 7 Slaves) gleichzeitig aktiv sein. Der Master steuert die Kommunikation und vergibt die Sendeslots (TDM) an Slaves. Im Piconet können sich zusätzlich bis zu 255 Geräte im Ruhezustand befinden.

Mehrere Piconets (max. 10) können sich zu einam Scatternet zusammenschliessen. Dazu sind Bridges notwendig, die in beiden Netzen aktive Slaves sind. Im Jahre 200 sollen Produkte auf den Markt kommen, die diese Funktion übernehmen können.

Bluetooth-Verbindungsaufbau

Jedes Gerät hat eine eindeutige 48bit-Adresse und zusätzlich eine 24bittige Klassen-ID (Telefon, Headset, Computer etc.). Zur Identifikation wird jedoch meist ein selbst festgelegter Gerätename verwendet. Der Verbindungsaufbau erfolgt in 3 oder 4 Schritten:

1. irgendein Gerät schickt ein „inquiry“ um andere Geräte zu finden
2. jeder kann antworten (wenn so am jeweiligen Gerät eingestellt)
3. Einigung über Profile und die benutzten Kanäle ("channelsëntsprechen den Ports bei TCP/UDP)
4. eventuell Authentifizierung

Profile

Die Bluetooth-Spezifikation beschreibt eine große Anzahl an Anwendungsprofilen. Die Profile bei Bluetooth sind ein sehr komplexes Feld mit zum Teil inkompatiblen Profilen. Mit den Profilen wird festgelegt welche Dienste die Geräte dem Partner jeweils zur Verfüfung stellen und welche Daten und Befehle sie dazu benötigen. Der Austausch der Profile erfolgt nach dem Verbindungsaufbau. Es gibt zwei obligatorische Profile die jedes Gerät beherrschen muss und eine sehr große Anzahl optionaler Profile. Exemplarisch werden neben den obligatorischen Profilen zwei optionale Profile vorgestellt.

obligatorisch: "Generic Access Profile" verwaltet sichere Kanäle zwischen den Partnern, Basis für andere Profile

obligatorisch: "Service Discovery Profile" verwaltet Informationen über zur Verfügung stehende Dienste der Partner, Basis für andere Profile

optional: "Advanced Audio Distribution Profile" Stereo-Audio-Signale können drahtlos via Bluetooth an ein entsprechendes Empfangsgerät gesendet werden

optional: "SIM Access Profile" ist ein Handy-Protokoll, damit ist es möglich, mittels Bluetooth eine Verbindung mit der SIM-Karte eines Handys herzustellen

4 Wireless USB

Die Arbeitsgruppe IEEE 802.15.3a versuchte sich an der Standardisierung von UWB als Basis für Wireless USB. Leider gibt es beim Ersatz des Kabelgebundenen USB zwei konkurrierende Verfahren. Einmal das UWB-Forum mit dem Direct Sequence Spread Spectrum und die WiMedia-Alliance mit dem Multiband-Orthogonal Frequency Division Multiplexing. Die Standardisierungsbenühungen sind deshalb im Januar 2006 geplatzt. Laut Aussage der beiden Konkurrenten soll nun der Markt entscheiden. Dies könnte sich jedoch als trügerisch erweisen, da einerseits die europäischen Regulatoren in Bezug auf UWB sehr konservativ sind. Andererseits ist zu erwarten, dass die sich Verbraucher nach dem Kauf zweier nicht kompatibler Geräte enttäuscht abwenden werden. Zudem ist noch nicht geklärt, inwieweit sich bei einem Einsatz im gleichen Haushalt die beiden Techniken stören.

5 ZigBee

Nach Angaben der ZigBee Alliance stammt der Name „ZigBee" vom Tanz der Honigbienen ab, mit dem sie den anderen Koloniemitgliedern mitteilen, in welcher Richtung und Entfernung sich Futterquellen befinden. Die ZigBee Alliance schreibt:

> The domestic honeybee, a colonial insect, lives in a hive that contains a queen, a few male drones, and thousands of worker bees. The survival, success, and future of the colony is dependent upon continuous communication of vital information between every member

> of the colony. The technique that honey bees use to communicate new-found food sources to other members of the colony is referred to as the ZigBee Principle. Using this silent, but powerful communication system, whereby the bee dances in a zig-zag pattern, she is able to share information such as the location, distance, and direction of a newly discovered food source to her fellow colony members. Instinctively implementing the ZigBee Principle, bees around the world industriously sustain productive hives and foster future generations of colony members.[2]

Diese Namensgebung ist jedoch nach Ansicht der Biologen falsch und wahrscheinlich allein der Tatsache geschuldet, einen marketingfähigen Namen für das Produkt zu finden. Zur Kommunikation von Futterquellen benutzen Honigbienen statt dessen entweder einen Rundtanz oder einen Schwänzeltanz.[3] „CircleBee“ hat jedoch längst nicht den gleichen Klang wie „ZigBee“.

5.1 Geschichte

Nach der Entwicklung von Bluetooth und dessen Markteinführung stellte aus der Sicht verschiedener Firmen heraus, dass WiFi und Bluetooth für selbstorganisierende Ad-hoc-Netzwerke kleiner und einfacher Geräte und Sensoren nicht geeignet ist. Im Gegensatz zu WiFi bestand vor allem ein Bedarf nach geringen Datenraten und gegen Bluetooth sprach der immer noch zu hohe Endpreis der zugrundeliegenden Technik. Daher begann 1998 die Entwicklung eines neuen Standards für energiesparende, kabellos kommunizierende Endgeräte mit geringen Datenraten. Im Mai 2003 wurde mit dem Standard IEEE 802.15.4 „Low Rate WPAN“ die Grundlage für ZigBee geschaffen, der im März 2005 durch IEEE 802.15.4a „WPAN Low Rate Alternative PHY“ ergänzt wurde. Für September 2006 wird mit der Verabschiedung von IEEE 802.15.4b „Revisions and Enhancements“ gerechnet.[4]

Während die IEEE nur die physikalische Schicht (PHY) und die Subschicht für die Medienzugriffskontrolle (MAC) standardisiert hat, hat die ZigBee Alliance im Dezember 2004 die ZigBee-Spezifikation verabschiedet und sie im Juni 2005 für die Öffentlichkeit verfügbar gemacht.[5]

Für den Zugang zur ZigBee-Spezifikation bedarf es einer Mitgliedschaft in der ZigBee Alliance, die mindestens 3500$ pro Jahr kostet. Die öffentlich zugängliche Version darf – im Gegensatz zur Bluetooth-Spezifikation – nur für nichtkommerzielle Zwecke genutzt werden. Es kann daher sein, dass ZigBee ob seines proprietären Charakters der Erfolg von Bluetooth versagt bleibt.

5.2 Technische Grundlagen

Designziele

Die Ziele der ZigBee Alliance lauten nach eigenen Angaben:

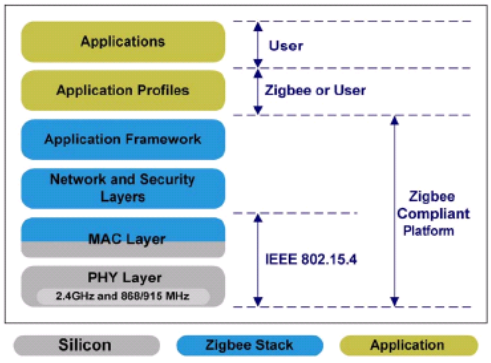
[2] http://zigbee.org/en/about/faq.asp#7
[3] http://de.wikipedia.org/wiki/Tanzsprache
[4] http://en.wikipedia.org/wiki/IEEE_802.15.4
[5] http://en.wikipedia.org/wiki/ZigBee

> The goal of the ZigBee Alliance is to create a specification defining mesh, peer-to-peer, and cluster tree network topologies with data security features and interoperable application profiles. The ZigBee specification provides a cost-effective, standards-based wireless networking solution that supports low data rates, low power consumption, security and reliability.[6]

Um den großen Markt drahtlos vernetzter Sensoren bedienen zu können, sollten ZigBee-Transmitter vor allem konkurrenzlos billig zu produzieren sein. Während Bluetooth-Chips in großen Stückzahlen derzeit zu einem Preis von etwa 3$ angeboten werden, liegt der Zielpreis von ZigBee-Chips bei unter 1$. Haupteinsatzgebiet von ZigBee sollen selbstorganisierende Ad-hoc-Netzwerke sein, in denen eine stabile und kryptographisch gesicherte Kommunikation zwischen den Endgeräten möglich ist, die darüber hinaus noch den Anforderungen weicher Echtzeit genügt. Dabei sollen sowohl vermaschte als auch Peer-to-Peer-Netzwerke aufgebaut werden können, die selbst wieder zu größeren so genannten Cluster-Bäumen verbunden werden können.[7] Trotz der großen kommunikationstechnischen Anforderungen an die Geräte soll der Energiebedarf minimal sein und damit noch weit unter dem Energiebedarf anderer drahtloser Technologien liegen.

Stack und Plattform

Während der Standard IEEE 802.15.4 die grundlegenden Eigenschaften der Hardware auf der physikalischen und der MAC-Schicht beschreibt, setzt der ZigBee-Stack darauf auf. Der „Network and Security Layer“ beinhaltet die Adressierung von ZigBee-Geräten und die Sicherheitsmechanismen auf der Netzwerkebene, wobei der Payload der ZigBee-Pakete verschlüsselt werden kann und grundsätzliche Authentifizierungsmöglichkeiten zur Verfügung gestellt werden. Im Application Framework sind verschiedene Primitiven definiert, mit denen ein ZigBee-Gerät ein Netzwerk gründen, einem solchen beitreten bzw. es wieder verlassen kann; sowie einige Verwaltungs-Primitiven wie „get“ und „set“ für Eigenschaften, die in der PAN Information Database gespeichert werden können.



http://www.eetimes.com/showArticle.jhtml?articleID=173600329

[6] http://zigbee.org/en/about/faq.asp#3
[7] http://en.wikipedia.org/wiki/ZigBee

Technologie

Frequenzbereiche: Grundsätzlich nutzt ZigBee das 2,4 GHz ISM-Band zur Kommunikation, allerdings kann als Fallback auch der Bereich um 868 MHz (in Europa) und 915 MHz (in den USA) genutzt werden.

Kanäle: Im 2,4 GHz Bereich nutzt ZigBee 16 Kanäle mit einer Bandbreite von je 5 MHz. Ein weiterer Kanal ist ZigBee in Europa im 868 MHz Bereich zugewiesen, und in den USA kann ZigBee im Fallback-Bereich weitere 10 Kanäle nutzen.

Sendeleistung: Die Sendeleistung von ZigBee-Geräten soll bei etwa $1 - 10$ mW liegen.

Reichweite: Laut ZigBee Alliance liegt die theoretische Reichweite bei etwa 100 m. Realistisch kann jedoch mit einer maximal erreichbaren Reichweite von ungefähr $50 - 70$ m gerechnet werden.

Datenrate: Die Datenrate beträgt im 2,4 GHz Bereich etwa 250 kbit/s pro Kanal, etwa 40 kbit/s pro Kanal im Bereich von 915 MHz und 20 kbit/s im 868 MHz-Bereich.

Datenkodierung : Zur Kodierung der Daten wird mit Direct Sequence Spread Spectrum (DSSS) ein Frequenzspreizverfahren verwendet.

Modulationsverfahren : Das Signal wird phasenmoduliert – im Bereich von 868 MHz und 915 MHz wird Binary Phase-shift Keying (BPSK) und im Bereich von 2,4 GHz Quadrature Phase-shift Keying (QPSK) verwendet. BPSK überträgt dabei 1 Bit pro Symbol, während es bei QPSK 2 Bits pro Symbol sind.

Devices und Rollen

Für die Nutzung von ZigBee sind zwei verschiedene Device Types definiert: Full Function Devices (FFD) und Reduced Function Devices (RFD). Hersteller sind verpflichtet, erstere mit einem vollständigen ZigBee-Stack auszustatten. Für letztere genügt es, nur eine Teilmenge dieses Stacks zu implementieren, so dass die Software für RFDs nur ein Fünftel bis ein Viertel des Umfangs einer vollständigen Implementation umfasst.

ZigBee-Geräte können drei verschiedene Rollen annehmen. Jedes Gerät – ob FFD oder RFD – ist ein ZigBee End Device (ZED) und muss nur in der Lage sein, sich an einem ZigBee Router (ZR) anmelden zu können. ZigBee End Devices bilden mit je einem ZigBee Router ein Netzwerk in Stern-Topologie. ZigBee Router (ZR) müssen notwendig FFDs sein. Sollte bei ihrer Initialisierung bereits ein anderer Router existieren, melden sie sich dort an und bilden danach mit anderen Routern entweder ein Netzwerk in Baum-Topologie oder ein vermaschtes (Mesh-) Netzwerk. Genau ein Router in einem WPAN – so es sich um ein „beacon enabled network“ handelt – übernimmt zusätzlich die Rolle des ZigBee Coordinators (ZC). Dieses Gerät gibt danach die grundlegenden Netzwerkparameter vor und verwaltet die ACLs und die Schlüssel für das gesamte WPAN. Der ZigBee Coordinator muss selbstverständlich auch ein FFD sein.

In verschiedenen Quellen werden die Rollen unterschiedlich benannt. Möglich scheinen dabei folgende zwei Benennungsmuster:

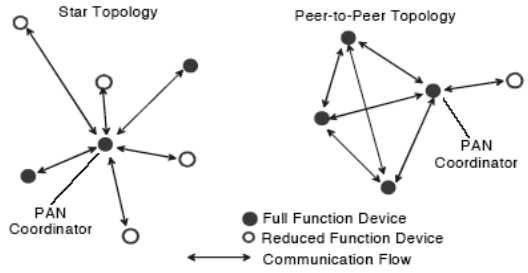
1. ZigBee End Device – ZigBee Router – ZigBee Coordinator
oder
2. ZigBee End Device – ZigBee Coordinator – PAN Coordinator.

5.3 Grundlagen der Kommunikation

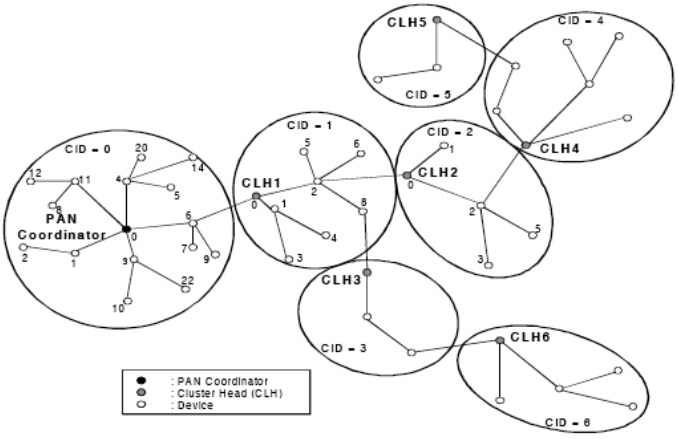
Topologien

ZigBee unterstützt drei verschiedene Netzwerk-Topologien. ZEDs können mit ZR ein sternförmiges Netzwerk bilden während ZRs auch in der Lage sind, Peer-to-Peer-Netzwerke (vermaschte oder Mesh-Netzwerke) aufzubauen. Diese können dann wieder zu größeren Netzwerken erweitert werden, die in der ZigBee-Nomenklatur als Cluster-Bäume bezeichnet werden. Die ZRs in den einzelnen Clustern agieren dann als Bridges bzw. Router zwischen den Clustern, wobei diese dann als Cluster Heads bezeichnet werden und jeweils in beiden Clustern aktiv sind. Einer der ZRs wird dann zum ZigBee Coordinator und ist damit der zentrale Knoten im Cluster-Baum.

Ein ZigBee-Netzwerk kann aus maximal 255 Clustern bestehen, die selbst wieder maximal 254 Nodes besitzen können. Daraus folgt, dass ein ZigBee-Netzwerk insgesamt maximal 64770 Geräte umfassen kann.



http://www.nflora.dk/studie/wp-content/uploads/presentation.ppt



http://www.nflora.dk/studie/wp-content/uploads/presentation.ppt

Adressierung

Ein ZigBee-Gerät besitzt zwei Adressen: eine 64 Bit lange Adresse, mit der das Gerät sich anmeldet, und eine 16 Bit lange Adresse, die dann innerhalb eines

Netzwerkes für die Kommunikation untereinander genutzt wird, um dadurch den Overhead zu reduzieren.

Ein bestimmter Dienst auf einem ZigBee-Gerät wird durch die Kombination von Adresse und Endpoint angesprochen. Ein Endpoint entspricht dabei in etwa den Ports bei TCP/IP, jedoch mit zwei großen Unterschieden. Erstens können nur 255 verschiedene Endpoints direkt genutzt werden, zweitens sind Dienste nicht fest mit Endpoints verknüpft, d. h. es existieren keine so genannten „well known ports".

Endpoint 0: Fest definiert für Management-Aufgaben. Über diesen Endpoint können z. B. die angebotenen Dienste von anderen Geräten abgefragt werden.

Endpoints 1 – 240: Frei verfügbar.

Endpoints 241 – 254: RFU – Reserved for Future Use – Reserviert.

Endpoint 255: Broadcast-Endpoint: Da jedes Gerät einen anderen Endpoint für einen bestimmten Dienst benutzen kann, ist es nicht möglich, einfach einen bestimmten Dienst auf allen ZigBee-Geräten im Netzwerk anzusprechen, wie dies z. B. bei der Kommunikation über IP gemacht wird. Statt dessen müssen in einem solchen Fall alle Geräte im Netzwerk auf ihrem Broadcast-Endpoint angesprochen werden.

Es gibt zwei verschiedene Übertragungsmodi: die direkte und die indirekte Übertragung. Bei der direkten Übertragung werden die Daten einfach während der Contention Access Period (CAP) gesendet und gelangen direkt zum Empfänger. Eine indirekte Übertragung findet statt, wenn das Zielgerät gerade nicht aktiv ist oder sich aus einem anderen Grund gerade nicht im Empfangsmodus befindet. In diesem Fall werden die Daten in eine so genannte „indirect transmission queue" eines aktiven Gerätes geschickt. Dabei sollte das Gerät selbst ein Router sein, weil damit die Wahrscheinlichkeit gering ist, dass es selbst lange inaktive Perioden besitzt. Damit die ZEDs wissen, dass sie diese Queue in einem Poll-Verfahren abfragen sollen, werden sie über das Beacon durch den Coordinator über die wartenden Nachrichten informiert. In Non-Beacon-Netzwerken wird von den ZEDs einfach die Primitive „poll" genutzt, da es ja keine Beacons gibt, die die wartenden Nachrichten anzeigen können.

Protokolle

ZigBee benutzt zwei verschiedene Protokolle: eines mit Beacons und eines ohne.

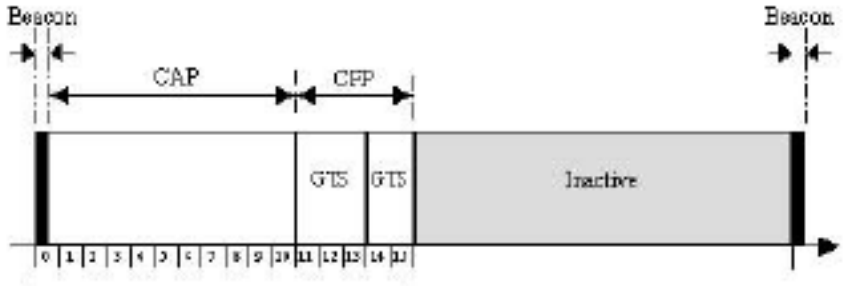
In Netzwerken ohne Beacons wird ein CSMA/CA-Mechanismus genutzt. Dabei wird auf dem als frei erkannten Übertragunsgkanal ein Clear Channel Assessment (CCA) gesendet. Stellt sich dann heraus, dass der Kanal doch nicht frei ist, wartet das sendende Device eine zufällige Zeit ab, bevor es erneut zu senden versucht. In solchen Netzwerken sind ZRs im Prinzip immer empfangsbereit, weil sie oftmals eine bessere Energieversorgung haben, während ZEDs nur senden, wenn ein Ereignis (z. B. ein Tastendruck) aufgetreten ist.

Im Beacon-Modus senden die ZR in periodischen Abständen Beacons. Durch diese Beacons wird eine Art komplexer Zeitschlitze geschaffen, eine so genannte Superframe-Struktur. Ein Superframe beginnt immer mit einem Beacon. Darauf folgt die Contention Access Period (CAP), in der die Kommunikation wie

im Non-Beacon-Modus abläuft, also unter Verwendung von CSMA/CA. Anschließend folgt die Contention Free Period (CFP), die wiederum in Guaranteed Time Slots (GTS) unterteilt ist, also nach dem TDMA-Verfahren (Time Division Multiple Access) funktioniert. Die einzelnen Zeitschlitze werden für die Kommunikation zwischen den Geräten benutzt, wobei durch das Beacon vorher festgelegt wurde, welches Gerät wann senden darf. Dadurch kann weiche Echtzeit garantiert werden. Am Ende eines jeden Superframes folgt die Inactive Period, in der die ZEDs „schlafen“ können. Die Cluster Heads nutzen diese Zeit zur Kommunikation mit den anderen Cluster Heads, wobei die Inactive Period aus der Sicht der Cluster Heads wiederum eine Superframe-Struktur besitzt.

Timing

Es gibt sehr hohe zeitliche Anforderungen an Sende- und Empfangs-Operationen. Die Turn-Around-Zeit beträgt 192 μs vom Beginn des Sendens bis zum Ende des Empfanges. Da das Filtern der Frames extrem zeitkritisch ist, muss die Bearbeitung von Frames sofort gestoppt werden, wenn ein Frame durch den Filter fällt. Andernfalls muss ein Gerät im Non-Beacon-Modus spätestens 192 μs, nachdem das letzte Byte eines gültigen Frames empfangen wurde, das ein ACK verlangt, das ACK auch senden. Im Beacon-Modus werden die ACKs mit den Beacons mitgeschickt. Dass dies funktioniert, liegt daran, dass RFD nur zum Senden von Daten vorgesehen sind und dadurch selbst nie ACKs senden müssen.



http://www.nflora.dk/studie/wp-content/uploads/presentation.ppt

5.4 ZigBee im Netzwerk

Ein ZigBee-Gerät unterstützt, zumindest wenn es sich um ein FFD handelt, drei verschiedene Scan-Typen in vier Varianten. Die drei Scan-Typen sind:

aktiver Scan: Das Gerät sendet einen Frame und wertet die Antwort aus.

passiver Scan: Der Empfänger wird für eine bestimmte Zeitspanne aktiviert und wertet jeden validen Verkehr aus.

Energie-Scan: Das Gerät misst das Energie-Niveau auf den angegebenen Kanälen.

Die vier Scan-Varianten sind in IEEE 802.15.4 definiert. Dabei kann entweder aktiv oder passiv nach Beacons gescannt werden oder aktiv nach so genannten „orphan notifications“. Alternativ kann das Gerät einen Energie-Scan durchführen.

Aufbau eines PAN

Bevor ein ZigBee-Gerät ein neues Netzwerk aufbauen kann, muss es zuerst einen Energie-Scan durchführen und dann den Kanal wählen, der das geringste Energie-Niveau aufweist, und damit auch den geringsten Traffic. Das ZED, das ein PAN mit der Primitive „start“ startet, wechselt seine Rolle zum ZigBee Coordinator. Ein ZED, das später die Primitive „start“ benutzt, wird dadurch zum ZigBee Router in diesem Netzwerk und benutzt den gleichen Kanal und die gleiche PAN-ID (die Netzwerkkennung) wie der ZigBee Coordinator.

Beitritt zu einem PAN

Bevor ein ZigBee-Gerät mit anderen Geräten kommunizieren kann, muss es dem PAN beitreten. Dazu nutzt es eine Primitive „associate“. Der ZigBee Coordinator entscheidet dann über die Aufnahme des ZEDs in das PAN. Der IEEE-Standard legt jedoch nicht fest, auf welcher Grundlage der ZC diese Entscheidung treffen muss.

Um sich von einem PAN abzumelden, nutzt ein Gerät die Primitive „disassociate“. Diese Primitive kann auch vom ZC genutzt werden, um ein Gerät aus dem Netzwerk auszuschließen.

Verwaiste Geräte

Ein ZigBee-Gerät wird als verwaist bezeichnet, wenn es Teil eines Netzwerkes war und den Kontakt zum Netzwerk verloren hat. Dies kann z. B. während oder nach einer Inactive Period passieren. Das ZED führt dann einen aktiven Scan nach „orphan notifications“ durch und fragt dabei bei den ZR nach, ob dort jeweils Nachrichten an sich liegen, die es mittels Poll-Verfahren abrufen kann. Wenn es bereits Teil des ZigBee-PANs war, tritt ein solcher Fall mit hoher Wahrscheinlichkeit irgendwann ein. Dadurch erfährt dann das ZED, dass es zu einem PAN gehörte und zu welchem genau. Danach ist es wieder Teil des Netzwerkes. Ob sich daraus mögliche Sicherheitsprobleme ergeben, wird sich nur durch Überprüfung konkreter Implementierungen zeigen lassen.

PAN-Konflikte

Es kann vorkommen, dass zwei benachbarte Netze die gleiche PAN-ID verwenden. Dieser Fall wird als PAN-Konflikt bezeichnet. Wenn ein Gerät einen Konflikt bemerkt, muss es den eigenen ZC davon in Kenntnis setzen. Der ZC muss dies an eine höhere Schicht im Software-Stack weitergeben, die sich dann um die Konfliktlösung kümmern muss. Auch hier ist wieder nur dieser Teil des Weges im Standard definiert, nicht jedoch, welche Konfliktlösungen möglich sind und welche gewählt werden sollen bzw. explizit nicht gewählt werden sollen. Hierbei handelt es sich um eine theoretische Lücke des Standards, die sich eventuell für einen DoS-Angriff ausnutzen lässt.

PAN Information Database (PIB)

In der PIB werden alle Einstellungen für den Medienzugriff gespeichert. Auf diese Einstellungen kann von außerhalb des ZigBee-Stacks mit den Primitiven „set“ und „get“ zugegriffen werden.

5.5 ZigBee und Sicherheit

ZigBee bietet drei grundsätzliche Mechanismen für sichere Datenübertragungen an: ACLs, Verschlüsselung auf der Basis von AES und Packet Freshness Timer.

Der ZigBee Coordinator führt eine Access Control List (ACL), in der für jede Adresse die verwendete Sicherheitsstufe sowie weitere Informationen bzgl. dieser Stufe gespeichert werden. Die ACL hat jedoch nur 256 Einträge, davon 255 für individuelle Adressen sowie ein Eintrag für alle unbekannten Adressen. Die vier Sicherheitsstufen sind:

- keine Sicherheit
- Vertraulichkeit
- Authentifikation
- Vertraulichkeit und Authentifikation.

Dabei bedeutet Vertraulichkeit, dass der Payload der MAC-Frames verschlüsselt wird. Die erweiterten Informationen in der ACL beinhalten dann den verwendeten Schlüssel. Als Verschlüsselungsverfahren kommt der Advanced Encryption Standard (AES) mit einer Schlüssellänge von 32, 64 oder 128 Bit zum Einsatz, d. h. ein symmetrisches Verfahren. Möglich sind sowohl Peer-to-Peer- als auch Gruppen-Schlüssel, allerdings bedeuten Gruppen-Schlüssel, dass mehrere Einträge in der ACL den gleichen Schlüssel zugewiesen bekommen. Dabei handelt es sich um eine Schwachstelle von ZigBee.

Jedes Gerät besitzt einen Packet Freshness Timer. Damit überprüft es bei allen empfangenen Paketen den Frame Counter. Zeigt der Frame Counter, dass es sich um ein älteres Paket handelt, wird dieses verworfen. Es handelt sich hier demnach um einen Versuch, Reply-Attacken zu verhindern. Sollte es gelingen, einem Empfänger ein Paket mit einem sehr hohen Frame Counter unterzuschieben, ist der Sender danach nicht mehr in der Lage, mit dem Empfänger zu kommunizieren, weil dieser jedes Paket als bereits abgelaufen betrachtet. Dies kann – abhängig von der konkreten Implementation – für einen Denial of Service Angriff ausgenutzt werden.

Risiken und mögliche Angriffe

Neben den bereits erwähnten Angriffsmöglichkeiten sind uns zwei Sicherheitsprobleme besonders aufgefallen.

Erstens scheint es möglich zu sein, den unterdefinierten Umgang mit PAN-Konflikten (vgl. 5.4) auszunutzen. Dazu muss ein Angreifer den Netzwerkverkehr belauschen und die PAN-ID herausfinden. Dann sendet er auf der gleichen Frequenz Pakete mit der gleichen PAN-ID wie das anzugreifende Netzwerk. Der ZigBee Coordinator des angegriffenen Netzwerkes wird dann versuchen, den Konflikt zu lösen. Aus unserer Sicht kann er dies nur auf zwei Arten machen: entweder die PAN-ID wird geändert oder sie wird nicht geändert. Im zweiten Fall besteht die Gefahr, durch die Konkurrenz und die gegenseitigen Störungen die Verlässlichkeit des Netzwerkes zu verringern. Daher werden sich die meisten für den ersten Fall entscheiden und einen Konfliktlösungsmechanismus implementieren, bei dem sich der ZigBee Coordinator eine neue PAN-ID wählt. Da er diese PAN-ID den anderen Nodes im Netzwerk mitteilen muss, entsteht für

einen kurzen Zeitraum ein instabiles Netzwerk. Dies kann dann der Angreifer entweder ausnutzen, um sich selbst als neuer ZigBee Coordinator (z. B. auch mit der alten PAN-ID) zu präsentieren oder um einen Denial of Service Angriff durchzuführen, indem er immer wieder die PAN-ID ermittelt und einen erneuten Konflikt provoziert.

Das zweite Sicherheitsproblem liegt in der Verwendung von 32 Bit-Zahlen für Zeitangaben. Absolute Zeitangaben werden sekundengenau gespeichert und umfassen die Jahre 2000 bis 2187. Relative Zeitangaben hingegen speichern die Werte in Millisekunden, daher tritt der Überlauf bereits bei etwas mehr als 49 Tagen auf. Für einen Sensor kann dies durchaus nur ein sehr kurzer Abschnitt in seinem Lebenszyklus sein. Bei PCs hieß dieses Problem vor einiger Zeit Y2K-Problem, und eigentlich sollten es die ZigBee-Entwickler besser wissen.

6 Ausblick

(Nicht nur) Aus unserer Sicht werden Wireless Personal Area Networks immer wichtiger. Sie werden im Sinne des „ubiquous computing“ (auch „pervasive computing“ genannt – also „unmerklich“ oder „durchdringend“) einen großen Bereich abdecken. Ohne uns wahrsagerische Fähigkeiten anmaßen zu wollen, glauben wir doch, uns einige Vorhersagen über die angesprochenen Technologien erlauben zu können.

UWB: Durch die Nutzung einer extremen Bandbreite kann es passieren, dass UWB das gleiche Schicksal ereilt wie die Funkentechnik zu Beginn des 20. Jahrhunderts und eine folgende strenge Limitierung der Sendeleistung negativen Einfluss auf die zu erreichende Datenrate hat.

Bluetooth: Die Technologie ist gut am Markt eingeführt und da bereits viele Mobiltelefone mit Bluetooth ausgestattet sind und diese immer mehr mit Multimedia-Fähigkeiten ausgestattet werden, steht Bluetooth durchaus in dem Ruf, eine Multimedia-taugliche Technologie zu sein. Die beabsichtigten Erweiterungen hin zu einer höheren Datenrate werden diesen Ruf weiter festigen.

Wireless USB: Der Streit zwischen den Vertretern der beiden konkurrierenden Technologien für WUSB hat bisher eine Markteinführung verhindert. Sollte sich an dieser Situation kurzfristig nichts ändern, wird WUSB nur schwer mit Bluetooth konkurrieren können.

ZigBee: ZigBee ist hervorragend für kleine und billige Geräte und geringe Datenraten geeignet. Vor allem Sensoren- und Hausautomationssysteme scheine kurzfristig marktreif zu sein. Sollte es den Herstellern gelingen, die von uns (punktuell) aufgezeigten Sicherheitsprobleme zu lösen, dürfte einer weiten Verbreitung nur wenig entgegenstehen.

7 Projekt

Bisher gibt es nur wenige fertige Systeme, die auf dem ZigBee-Stack aufbauen, für Endkunden zu laufen. Neben einigen Praxistests sollen angeblich die ersten Systeme den Markt erreicht haben. Ein Beispiel dafür ist die „Verschönerung“

von Autorädern, die mittels LEDs Bilder projezieren können, wobei die Bilddaten mittels ZigBee an den Controller geschickt werden.[8] Zu den Praxistest gehört eine Echtzeit-Überwachungsfunktion für Luftfeuchtigkeit, Temperatur und Lichtnutzung, die auf einem Netzwerk mit Stern-Topologie nach IEEE 802.15.4 aufbaut.[9]

7.1 Hardware

Wir haben vom Lehrstuhl Malek ein Entwickler-Kit für ZigBee zur Verfügung gestellt bekommen, das von der Firma Chipcon[10], einer Tochter von Texas Instruments, unter der Bezeichnung CC2431DK angeboten wird.

Folgende Hardware ist in dem Entwicklungs-Kit enthalten:

- 2 Entwickler-Boards (SmartRF04EB)
- 2 Entwickler-Module (CC2430EM)
- 10 Sockel-Boards (SOC_BB)
- 10 Entwickler-Module (CC2431EM)
- 12 Antennen

Die SmartRF04EB-Boards können über USB oder ein serielles Kabel an einen Rechner angeschlossen werden, von dem sowohl die Energie zur Verfügung gestellt wird als auch Software. Während die CC2430EM offensichtlich FFDs zu sein scheinen, handelt es sich bei den CC2431EM wohl um RFDs, die mit einer Software zur Positionsbestimmung ausgeliefert werden. Beide können jedoch mit Hilfe der mitgelieferten Software geflasht werden, so dass es sich auch bei den CC2431EM durchaus um FFDs handeln könnte. Alle Module können auf 128 kByte Flash-Speicher zugreifen.

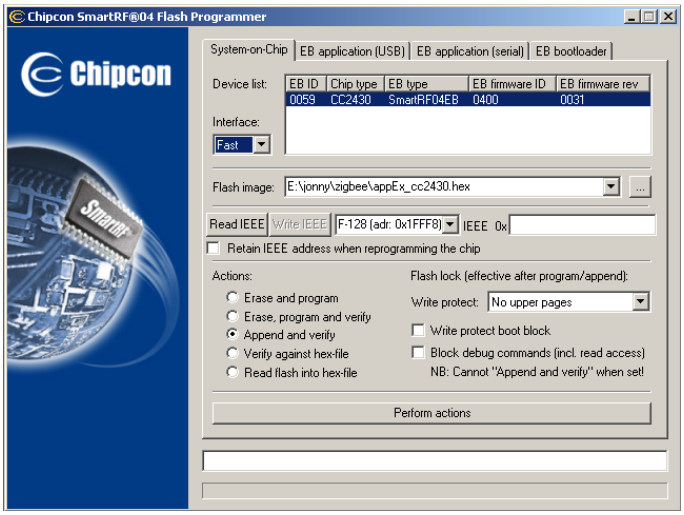
Da wir nicht allein auf die gesamte Hardware zugreifen konnten, waren wir in den Möglichkeiten der Nutzung stark eingeschränkt. Für eine Kommunikation zwischen zwei Geräten mit selbst aufgespielter Software hätten wir beide Geräte an verschiedenen Rechnern betreiben müssen, für eine Analyse des Datenverkehrs bräuchten wir gar drei Entwickler-Boards, weil die Geräte nicht gleichzeitig mit der gewählten Applikation und dem Sniffer arbeiten.

7.2 Software

Chipcon Flash Programmer

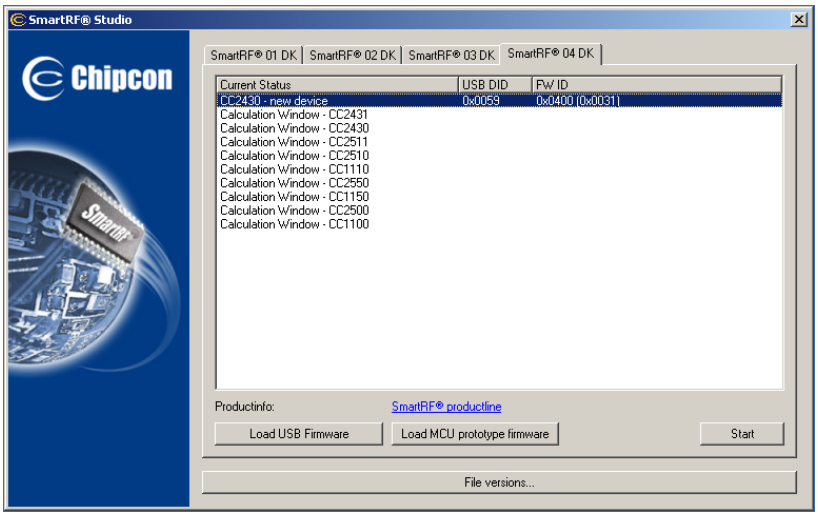
Wie der Name schon andeutet, dient das Programmm zum Flashen der Module. Auf diese Art können neue Programme direkt in den Speicher der Module geschrieben werden. Problematisch ist an diesem Programm, dass es nicht testet, ob die aufzuspielende Applikation einen Boot Loader besitzt oder nicht und auch nicht in der Lage ist, daie Applikation an die richtige Stelle im Speicher (nämlich genau nach dem Boot Loader) zu schreiben.

[8] http://www.bigwheels.net/promotion/pimpstar.html
[9] http://193.120.95.161/buildingmonitor/
[10] http://www.chipcon.com



SmartRF Studio for CC2420/2430/2431

Mit Hilfe dieser Software ist es möglich, die Flash-Speicher der Module auszulesen und auch direkt neu zu beschreiben, sowie die USB-Firmware der SmartRF04EB zu aktualisieren.

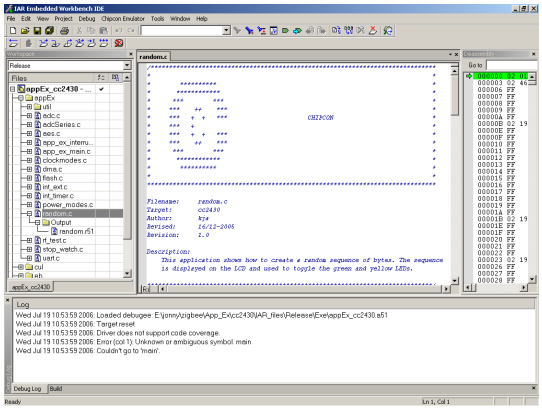


IAR Embedded Workbench

Hierbei handelt es sich um eine Integrierte Entwicklungsumgebung (IDE) für Intel 8051 Mikrocontroller von IAR Systems[11], mit der es auch möglich ist, eigene Software direkt aus der IDE auf die SmartRF04EB zu laden. Es werden ein paar Beispiel-Applikationen mitgeliefert, die dann direkt über das (eingeschränkte) Benutzer-Interface der SmartRF04EB gesteuert werden können. Dazu zählt z. B. das Senden und Empfangen von Testdaten sowie ein Test zur Ver- und Entschlüsselung. Da uns nur ein Entwickler-Board zur Verfügung stand,

[11] http://www.iar.com

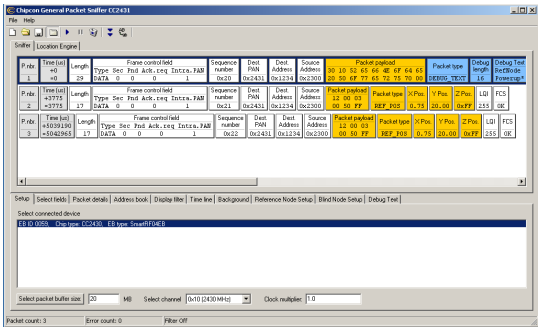
konnten wir die Kommunikation zwischen den Entwickler-Boards mit Hilfe der aufgespielten Programme erst nach Projektende testen (als wir mit tatkräftiger Hilfe von Johannes die falsch geflashten Module wieder in Ordnung brachten). Da uns dabei ein drittes Board fehlte, konnten wir die Kommunikation zwischen den Borads nicht mitsniffen, da sich Programmausführung und Sniffen auf dem gleichen Board ausschließen.



Chipcon General Packet Sniffer

Mit Hilfe des Sniffers können alle empfangenen Pakete angezeigt und analysiert werden. Leider ist das gleiche nicht auch für die gesendeten Pakete möglich. Dazu bedürfte es eines zweiten Entwickler-Boards an einem anderen Rechner. Außerdem lässt sich mit Hilfe der auf den Modulen installierten Software eine Positionsbestimmung der Module durchführen. Dabei wird den einigen Modulen (den Referenz-Modulen) mitgeteilt, an welcher Position sie sich befinden. Diese Positionsdaten werden dann von den Modulen als Payload der Pakete an das Entwickler-Board zurückgesendet. Anhand der Dämpfung lässt sich dann für weitere Module deren Position feststellen, indem Richtung und Dämpfung in Abhängigkeit von den Referenz-Knoten interpoliert wird. Die Positionsbestimmung wird dabei stark von eventuellen Störungen (z. B. durch sich bewegende Objekte oder Personen) beeinflusst, sie ist also keinesfalls genau.

In der folgenden Abbildung sieht man die ersten drei Pakete eines Referenz-Knoten an das Entwickler-Board. Zuerst teilt der Knoten mit, dass er gestartet wurde. Im Anschluss daran erhält er vom Entwickler-Board die im zugewiesenen Positionsdaten (dieses Paket wird nicht dargestellt). Danach sendet der Referenz-Knoten in bestimmten Abständen seine Positionsdaten.



Hier ist ein ZigBee-Daten-Paket (Data Packet) zu sehen, dessen Payload aus den Positionsdaten des Referenz-Knotens besteht.

P.nbr.	Time (us)	Length	Frame control field					Sequence number	Dest. PAN	Dest. Address	Source Address	Packet payload	Packet type	X Pos.	Y Pos.	Z Pos.	LQI	FCS
	+3775		Type	Sec	Pnd	Ack.req	Intra.PAN					12 00 03						
2	=3775	17	DATA	0	0	0	1	0x21	0x2431	0x1234	0x2300	00 50 FF	REF_POS	0.75	20.00	0xFF	255	OK

8 Literatur

IEEE Standard for Information technology: Telecommunication and information exchange between systems Local and metropolitan area networks – Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Computer Society, New York, NY, USA, October 2003,
http://standards.ieee.org/getieee802/802.15.html

ZigBee Alliance: http://zigbee.org
ZigBee FAQ: http://zigbee.org/en/about/faq.asp

Chipcon: http://www.chipcon.com

Jan Flora: 802.15.4 - An introduction, Department of Computer Science, University of Copenhagen, 15. Juni 2006,
http://www.nflora.dk/studie/wp-content/uploads/presentation.ppt

Bob Heile: ZigBee Alliance Tutorial, November 2005,
http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=6704

Khanh Tuan Le: ZigBee SoCs provide cost-effective solutions,
http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=7142

Patrick Kinney: ZigBee Technology: Wireless Control that Simply Works. October 2003,
http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=5162

Rui Silva, Serafim Nunes: Security Issues on ZigBee, 2005,
http://rtcm.inescn.pt/fileadmin/rtcm/WorkShop_22_Jul_05/
s2_Security_Issues_on_ZigBee.pdf

Wikipedia: http://de.wikipedia.org/wiki/Personal_Area_Network
http://en.wikipedia.org/wiki/Personal_Area_Network
http://de.wikipedia.org/wiki/Wireless_Personal_Area_Network
http://en.wikipedia.org/wiki/IEEE_802.15
http://en.wikipedia.org/wiki/Bluetooth
http://de.wikipedia.org/wiki/Bluetooth
http://en.wikipedia.org/wiki/Wireless_USB
http://de.wikipedia.org/wiki/Tanzsprache
http://en.wikipedia.org/wiki/IEEE_802.15.4
http://de.wikipedia.org/wiki/ZigBee
http://en.wikipedia.org/wiki/ZigBee

Sonstige Ressourcen: http://www.chipcon.com
http://www.tutorial-reports.com/wireless/zigbee
http://www.elektroniknet.de/topics/kommunikation/fachthemen/2004/0002/
http://www.elektroniknet.de/topics/kommunikation/fachthemen/2005/0005/
http://www.maxstream.net/wireless/zigbee.php
http://www.bluetooth.com
http://www.palowireless.com/infotooth/tutorial.asp